

Sophos Enterprise Console 5.3.0

Guia:

Manual de instalação do Sophos Enterprise Console 5.3.0

Versão 1

Data do Documento: Maio de 2015



Conteúdo

| 1. | Sob | re este manual | 3 |
|----|------|------------------------------------|----|
| 2. | Req | uisitos de Instalação | 4 |
| 3. | Inst | alando o Sophos Enterprise Console | 5 |
| 4. | Con | figurações recomendadas | 19 |
| 2 | l.1. | Anti-virus and HIPS | 19 |
| 2 | 1.2. | Firewall | 22 |
| 2 | 1.3. | Tamper protection | 23 |
| 2 | 1.4. | Patch | 24 |
| 5. | Inst | alando os endpoints (deploy) | 25 |
| | | | |



1. Sobre este manual

Este manual descreve os procedimentos necessários para realizar a instalação do Sophos Enterprise Console 5.3.0.

Com o Sophos Enterprise Console, é possível gerenciar todos os computadores protegidos pelo Sophos Endpoint, possibilitando inclusive o gerenciamento de diferentes sistemas operacionais e versões usando apenas uma interface.



2. Requisitos de Instalação

- 2.1. Requisitos para instalar o Sophos Enterprise Console: http://www.sophos.com/en-us/support/knowledgebase/118635.aspx
- 2.2. Requisitos para instalar o Sophos Antivírus nos computadores da rede:
- 2.2.1. Windows: <u>http://www.sophos.com/en-us/support/knowledgebase/118621.aspx</u>
- 2.2.2. Linux: http://www.sophos.com/en-us/support/knowledgebase/118624.aspx
- 2.2.3. Mac OS X: <u>http://www.sophos.com/en-us/support/knowledgebase/118623.aspx</u>
- 2.2.4. NetApp: <u>http://www.sophos.com/en-us/support/knowledgebase/118633.aspx</u>
- 2.2.5. UNIX: http://www.sophos.com/en-us/support/knowledgebase/118625.aspx



3. Instalando o Sophos Enterprise Console

- 3.1. Faça download e execute o arquivo "sec_530_sfx.exe", link para download: http://downloads.m3corp.com.br/sophos10/sec_530_sfx.exe
- 3.2. Clique no botão "Install".

| 📊 Sophos Enterp | rise Console 5.3.0 |
|-----------------|---|
| SOPHOS | This download contains Sophos Enterprise Console 5.3.0 and Sophos Update Manager 1.5.5. |
| | This allows you to deploy and manage Sophos Endpoint Protection across your network for Windows, Mac OS X, Linux, UNIX, VMware vShield. |
| | See the release notes for full system requirements. |
| | Destination folder Image: State Image: State |
| | Installation progress |
| | Install Cancel |

- 3.3. Aguarde enquanto os arquivos de instalação são extraídos.
- 3.4. Clique no botão "Avançar".





3.5. Clique em "I accept the terms in the license agreement" e clique no botão "Avançar".

| 📶 Sophos Enterprise Console 5.3.0 Installer | × |
|---|---|
| License Agreement Please read the following license agreement carefully. | 1 |
| SOPHOS END USER LICENSE AGREEMENT Please read the following legally binding License Agreement between Sophos and Licensee carefully. By selecting the accept option, breaking the seal on the software package, or installing, copying or otherwise using the Products, Licensee acknowledges that Licensee has read, understands, and agrees to be bound by the terms and conditions of this License Agreement, including without limitation the terms and conditions of documents and policies which are incorporated herein by reference. If Licensee does not agree with the terms and conditions of this License Agreement, Licensee is not authorized to install or otherwise use the Products. If accept the terms in the license agreement I do not accept the terms in the license agreement | |
| < Back Next > Cancel | |

3.6. Verifique se as três opções estão selecionadas e clique em "Avançar".

| 📶 Sophos Enterprise Console 5.3.0 Installer | × |
|--|-------------|
| Components Selection Select the components you want to install on this computer. | <u>lılı</u> |
| Management Console Manages Sophos software on networked computers. | |
| Management Server Handles updating and communication for Sophos software on networked computers. | |
| Database Stores security status data. | |
| < Back Next > | Cancel |



3.7. Caso algum item crítico for detectado, o item será sinalizado com o símbolo ⁽²⁾, itens críticos devem ser corrigidos antes de prosseguir com a instalação. Em caso de dúvida sobre algum item listado, verifique o artigo 113945 da Sophos (<u>http://www.sophos.com/support/knowledgebase/article/113945.html</u>)

| nii Sophos Enterprise Console 5.3.0 Installer |
|--|
| System Property Checks Sophos Enterprise Console has checked the properties of your system. |
| The Computer Browser service is not running on this computer. The "discover comput" The computer name exceeds 15 characters. The name might appear truncated in the The computer has multiple network adapters. The Management Server may not be at You are an administrator on this computer. The SYSTEM account can impersonate other accounts. The computer does not need to be restarted. The computer has at least 2 GB RAM. The operating system can support more than 4000 clients. Sophos Remote Management System is not installed. The computer Management System is not installed. |
| < Back Next > Cancel |

3.8. Na tela "Destination Folder", clique no botão "Avançar".

| 📶 Sophos Enterprise Console 5.3.0 Installer | X |
|---|--------------------------------|
| Destination Folder Click Next to install to this folder, or click Change to | install to a different folder. |
| Install the selected components to: | Change |
| Space Required: 410.19 MB Space Available: 81.43 GB | |
| < B. | ack Next > Cancel |



- 3.9. Na tela "Database Details", selecione a opção "Create a new instance called 'SOPHOS'".
- 3.10. Clique no botão "Browse".
- 3.11. Caso o computador esteja em um domínio no entanto o computador **não** é o "domain controller" (servidor do Active Directory):
 - 3.11.1. Clique no botão "Locais".
 - 3.11.2. Selecione o nome do computador onde a instalação está sendo executado.
 - 3.11.3. Clique no botão "OK".
- 3.12. Informe o usuário "SophosManagement" e clique no botão "OK".
- 3.13. Em "Password", informe: !s0ph0sMGR!
- 3.14. Clique no botão "Avançar".

| 📶 Sophos Enterprise (| Console 5.3.0 Installer | × |
|---|---|------------|
| Database Details Specify the user a | account for database access. | |
| Select the SQL Se database. | rver instance on your local computer to be used by the Sophos | |
| 🔿 Use an <u>e</u> xistin | g instance: | - |
| Create a new | instance called 'SOPHOS' | _ |
| | | |
| Specify the user a | account for database access. For more information, <u>Article 11395</u> | <u>4</u> . |
| User name: | MT-SRV-04\SophosManagement Browse | |
| Password: | ••••• | |
| | | |
| | < <u>V</u> oltar <u>A</u> vançar > Ca | ancelar |

3.15. Caso o ".NET Framework 4" não esteja instalado, o wizard de instalação irá realizar a instalação do mesmo. Neste caso clique no botão "Install".

| 📶 Sophos Enterprise Console 5.3.0 Installer | × |
|--|------|
| Install Required Software Sophos Enterprise Console will install Microsoft .NET 4. | |
| Microsoft .NET 4 will be installed automatically. Microsoft .NET 4 is needed to run the Management Server. | |
| After installation of Microsoft .NET 4, the computer must be restarted before continuing with the Sophos Enterprise Console installation. | |
| Click Install to begin. | |
| To review or manage any of your installation settings, click Back. | |
| Click Cancel to exit the Installer. | |
| | |
| | |
| < ⊻oltar [nstall] Canc | elar |



3.16. Caso o ".NET Framework 4" tenha sido instalado, será solicitada a reinicialização do computador, clique em "Concluir" para reinicia-lo. Caso não queira reiniciar o computador neste momento, desmarque a opção "Restart now" e clique em "Concluir". Após reiniciar, volte para o <u>passo 3.4</u>.

OBS: Após reiniciar o computador, o instalador será executado automaticamente, caso o mesmo usuário seja usado no logon. Caso seja necessário executar o instalador manualmente, execute o arquivo "C:\sec_530\ServerInstaller\Setup.exe".

| 📶 Sophos Enterprise Console 5.3.0 Installer 🛛 🛛 🔀 | | |
|---|--|--|
| SOPHOS | Installation of Enterprise Console is ready to resume | |
| | Microsoft .NET 4 has been successfully installed. To continue installing Sophos Enterprise Console 5.3.0 you must restart the computer. The Enterprise Console installer will start again automatically. To restart now, click Finish. To restart later clear the box below and click Finish. | |
| | < <u>V</u> oltar Concluir Cancelar | |

- 3.17. O mesmo que ocorreu com o ".NET Framework 4" ocorrerá também com o requisito "Windows Installer 4.5", caso o mesmo não esteja instalado.
- 3.18. Na tela "Communication Setting", <u>altere a porta</u> para "8191" e clique no botão "Avançar".

| 📶 Sophos Enterprise Console 5.3.0 Installer | × |
|--|----------|
| Communication Setting Please select the port to connect to the Management Server. | |
| Enter the port that the Management Console will use to connect to the Manageme Server using HTTP: For more information, see <u>KB article 114182</u> . <u>P</u> ort number: (e.g. 80) | ent |
| 8191 | |
| | |
| < <u>V</u> oltar <u>A</u> vançar > C | lancelar |

- 3.19. Na tela "Sophos Update Manager Credentials", clique no botão "Browse".
- 3.20. Caso o computador esteja em um domínio, no entanto o computador não é o "domain controller" (servidor do Active Directory):



- 3.20.1. Clique no botão "Locais".
- 3.20.2. Selecione o nome do computador onde a instalação está sendo executado.
- 3.20.3. Clique no botão "OK".
- 3.21. Informe o usuário "SophosUpdateMgr" e clique no botão "OK".
- 3.22. Em "Password", informe: !s0ph0s!
- 3.23. Clique em "Avançar".

| 📶 Sophos Enterprise Console 5.3.0 Installer | × |
|--|------------|
| Sophos Update Manager Credentials Specify the account details for Sophos Update Manager. | <u>III</u> |
| Sophos Update Manager is the component that downloads and distributes updates your network. Specify an existing user name and password that endpoints will use by default to connect to Sophos Update Manager. This should be a low privilege account and its password must never change. For more information, see <u>KB article 113954</u> . <u>User name:</u> | on |
| MT-SRV-04\SophosUpdateMgr Browse Password: | |
| < <u>V</u> oltar <u>A</u> vançar > Ca | ncelar |

3.24. Na tela "Manage Encryption", marque a opção "Do not manage encryption" e clique em "Avançar.

IMPORTANTE:

A funcionalidade de Full Disk Encryption (SDE) já não está mais disponível para novas aquisições de produto.

O suporte a essa funcionalidade permanece até Março de 2016, porém somente para os clientes que já haviam adquirido o produto com essa funcionalidade antes da descontinuação.



3.25. Na tela "Feedback to Sophos", desmarque a opção "I agree" e clique em "Avançar".

| 📶 Sophos Enterprise Console 5.3.0 Installer | × |
|---|--------|
| Feedback to Sophos Please read the following carefully. | |
| Enterprise Console will send Sophos a report each week. This report will show the number of managed and unmanaged computers on your network, as well as information about the operating systems and Sophos products that are in use. For further details about the types of information collected and the way in which your information is processed, please refer to the Sophos End User License Agreement and the Sophos Privacy Policy located here: http://www.sophos.com/legal You can stop sending these weekly reports at any time by changing your Enterprise Console settings. | |
| | |
| < <u>V</u> oltar <u>A</u> vançar > Ca | ncelar |

3.26. Na tela "Ready to Install", clique no botão "Install" para iniciar a instalação.

| III Sophos Enterprise Console 5.3.0 Installer | × |
|--|----------|
| Ready to Install The Installer is ready to begin the installation. | |
| Click Install to begin. | |
| To review or manage any of your installation settings, click Back. | |
| Click Cancel to exit the Installer. | |
| NOTE: A new SQL Server instance called 'SOPHOS' will be created during the insta process. | allation |
| < <u>V</u> oltar Install | Cancelar |



3.27. Aguarde a instalação finalizar.

| II Sophos Enterprise Console 5.3.0 Installer Installing Sophos Enterprise Console The program features you selected are being installed | | | |
|---|---|----------|--|
| Installing Sophos Enterprise Console The program features you selected are being installed. | | | |
| | | | |
| | Please wait while Sophos Enterprise Console is installed. This may take several minutes. | | |
| | Status: Installing component: Microsoft Message Queuing | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | < <u>V</u> oltar <u>N</u> ext > | Cancelar | |

3.28. Após finalizar a instalação, será solicitado um logoff, clique no botão "Concluir", o logoff será realizado (em alguns casos pode se solicitado a reinicialização).

| 📶 Sophos Enterprise Cons | ole 5.3.0 Installer | × |
|--------------------------|---|---|
| SOPHOS | Installation of Sophos Enterprise Console 5.3.0 is complete | |
| | Sophos Enterprise Console 5.3.0 has been successfully installed. To ensure Sophos Enterprise Console runs correctly, you need to log off. To log off now, click Finish. To log off later clear the box below and click Finish. | |
| | < ⊻oltar Concluir Cancela | r |

3.29. Faça login no servidor, após isto o Sophos Enterprise Console irá iniciar automaticamente.



3.30. Na tela "Download Security Software Wizard", clique no botão "Cancelar".

| Download Security Software | e Wizard | × |
|----------------------------|--|---|
| SOPHOS | Welcome to the Download Security Software Wizard | |
| | This wizard will guide you through the process of downloading and automatically updating the security software you need. You will need the username and password supplied to you by Sophos. | |
| | To continue, click "Next". | |
| | < <u>Vo</u> ltar <u>Avançar</u> > Cancela | r |

3.31. Na tela de confirmação, clique em "Sim".





3.32. No menu bar, clique em "View" > "Update Managers (caso esta opção estiver desabilitada, pule para o próximo passo)."

| 🔟 S | ophos | Enter | prise Co | nsole | | | |
|-----------|---------------------|---------------|-----------------|-------------------|--------------|-----------------|-----------------|
| Eile | <u>E</u> dit | View | <u>A</u> ctions | <u>G</u> roups | Policies | Eve <u>n</u> ts | <u>S</u> ubscri |
| | Discos | ✓ En | dpoints | | | | |
| 1 | DISCO. | Up | date Mana | agers | | | |
| Cor | Compute 🗸 Dashboard | | | | | | |
| | | ✓ <u>T</u> or | olbar | | | | |
| <u>Ma</u> | anagec | ✓ <u>S</u> ta | itus Bar | | | | |
| Ur | manag | Boo | otstrap Lo | cations | | | |
| Co | nnecte | Sop | ohos Upda | ate <u>M</u> anag | jer Installe | er Locatio | n |

3.33. Clique com o Botão direito no servidor e clique em "View/Edit Configuration".

| Update managers | | | | |
|-----------------|--|------------------------------|-----------|--|
| Computer 🔺 | | Alerts | Errors | |
| MT-SRV-04 | | | | |
| | | <u>V</u> iew Update Manage | r Details | |
| | | Update Now | | |
| | | View/ <u>E</u> dit Configu | ration | |
| | | Comply with Configu | ration | |
| | | <u>A</u> cknowledge Alerts | | |
| | | ⊆opy Delete Select All | | |

- 3.34. Clique no botão "Add".
- 3.35. Em "Address", informe: http://sophosv530-srv01.m3corp.com.br
- 3.36. Em "Username", informe seu usuário de atualização (informado em sua licença).
- 3.37. Em "Password", informe a senha do seu usuário de atualização.
- 3.38. Clique no botão "OK".

| Source Details | × |
|--|---|
| <u>A</u> ddress (HTTP or UNC): | http://sophosv530-srv01.m3corp.com.br 💌 📴 Browse |
| <u>U</u> sername: | CLI_EM_EMPRESA |
| Password: | |
| If updates from the details here, Proxy settings | the above source are downloaded through a proxy server, enter |
| Use a proxy | / server to connect |
| Address: | P <u>o</u> rt: 0 |
| User <u>n</u> ame: | |
| Pass <u>w</u> ord: | <u>Ch</u> ange |
| | OK Cancel |



- 3.39. Clique novamente no botão "Add".
- 3.40. Em "Address", informe: http://sophosv530-srv01.m3corp.com.br:8089
- 3.41. Em "Username", informe seu usuário de atualização (informado em sua licença).
- 3.42. Em "Password", informe a senha do seu usuário de atualização.
- 3.43. Clique no botão "OK" para salvar a nova "Source".



3.44. Clique na guia/aba "Subscription", selecione o item "Recommended", clique no botão ">" e então clique no botão "OK".

| So | urces | Subscriptions Distribution Schedule Logging Advanced | |
|----|------------------|---|--|
| | -Softw Select | vare subscriptions the software subscriptions for this update manager to maintain: | |
| | <u>A</u> vailat | ble: Subscribed to: | |
| | | Recommended | |
| | L | >> | |
| | L | | |
| | L | | |
| | L | | |
| | L | | |
| | L | | |
| | | < | |
| | L | | |
| | I | | |
| | | View details | |



- 3.45. Na janela "Configure update manager", clique no botão "OK".
- 3.46. Duas mensagens serão exibidas (conforme os exemplos das imagens abaixo), clique no botão "Sim" e em seguida clique no botão "OK":

| Sophos Ei | nterprise Console | × |
|-----------|---|--------------------|
| ⚠ | It is not possible to determine if the source location http://sophosv530-srv01.m3corp.com.br has a direct network path to Sophos because t managed. Would you like to save the configuration anyway? | he location is not |
| | <u>Sim</u> <u>N</u> ão | |
| | Sophos Enterprise Console | |
| | The update location http://sophosv530-srv01.m3corp.com.br at the top of your updating hierarchy is not managed. It is not possible to verify if it is up to date. Please ensure that the location is up to date. | |
| | CK I | |

- 3.47. Clique com o botão direito no servidor e clique em "Update now".
- 3.48. Aguarde a coluna "Download status" alterar de "Downloading binaries" para "Last checked at: <data atual>" (isto pode demorar em torno de 1 a 2 minutos).

| Update managers | | | | |
|-----------------|--------|--------|--------------|----------------------|
| Computer name 🔺 | Alerts | Errors | Last updated | Download status |
| 😽 MT-SRV-04 | | | Never | Downloading binaries |

3.49. Clique com o botão direito do mouse no "Recommended" e clique em "View/Edit Subscription".





3.50. A janela "Software Subscription" irá abrir, na coluna "Platform" selecione as plataformas desejadas (onde o servidor do Sophos irá fazer o download dos arquivos de instalação para as plataformas selecionadas), clique no botão "OK".

| oftware Subscriptior | ı - Recommen | ded | | <u>_ 0 ×</u> |
|----------------------|------------------|------------|------------------------------------|--------------|
| Subscription name: | Recommended | | | |
| License family: E | indpoint Protect | ion Advanc | ed | |
| Platform | Version | Status | Features | |
| Windows | | | | |
| 🔽 Windows, Plea | Recommen 💌 | | Anti-virus, Host Intrusion Prevent | ion |
| Мас | | | | |
| MAC OS X 10.6+ | 9 Recomme | | Anti-virus, Device Control | |
| Managed vShield, Li | | | | |
| 🔲 Linux - Please | 9 Recomme | | Anti-virus | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | De | tails |
| | | | | |
| | | | ОК С | ancel |
| | | | | |

3.51. Clique no botão "OK".

| Sophos Enterprise Console |
|---|
| The update location http://sophosv530-srv01.m3corp.com.br at the top of your updating hierarchy is not managed. It is not possible to verify if it is up to date. Please ensure that the location is up to date. |
| <u> </u> |



3.52. Clique no botão "OK".

| J | Software Subscription | × | | | |
|--|----------------------------|---|--|--|--|
| You have modified the software subscription "Recommended" which i used by the updating policies and indirectly by the groups listed below | | | | | |
| | Updating policies: Groups: | - | | | |
| | ОК |] | | | |

- 3.53. A coluna "Download status" irá voltar a indicar "Downloading binaries", o primeiro update (onde será realizado o download dos arquivos de instalação para cada plataforma selecionada anteriormente), quando o download finalizar, a coluna "Download status" irá indicar "Last checked at: <data>", é necessário aguardar o download finalizar para:
 - Fazer a instalação do Sophos Endpoint nas estações.
 - Configurar algumas políticas como "Application Control" e "Data Control", que dependem de algumas informações que são coletadas via update.

| Update managers | | | | | |
|-----------------|--------|--------|-------------------|----------------------|--|
| Computer name 🔺 | Alerts | Errors | Last updated | Download status | |
| 🛼 MT-SRV-04 | | | 4/5/2015 14:04:39 | Downloading binaries | |

3.54. Para voltar a visualizar o painel dos "endpoints", clique em "View" > "Endpoints".





4. Configurações recomendadas

Neste item, será demonstrado às configurações recomendadas para novas implementações do Sophos, onde o foco é configurar o Sophos para não causar nenhum bloqueio indesejado, mantendo a proteção contra malwares. Após o período de implementação, é recomendado ativas os módulos do Sophos de forma gradual.

4.1. Anti-virus and HIPS



- 4.1.1. No Sophos Enterprise Console, expanda o item "Anti-virus and HIPS".
- 4.1.2. Clique duas vezes na política de Antivírus e HIPS a ser editada (ou clique com o botão direito e clique em "View/Edit Policy")
- 4.1.3. Em "Enable on-access scanning", clique em "Configure...".

| Anti-Virus and HIPS Policy - Default |
|--|
| Authorization |
| Messaging |
| Sophos Live Protection |
| On-access scanning |
| Enable on-access scanning Configure |
| Enable behavior monitoring Configure |
| Web protection |
| Block access to malicious websites: On |
| Download scanning: As on-access scanning |
| Scheduled scanning |
| Set up and manage scheduled scans: |
| Name |
| |
| Add |
| Extensions and Exclusions |
| Changes to "Exclusions" or "Extensions" settings also affect the "Full system scan" and default on-demand scans on the individual computers. |
| OK Cancel |



4.1.4. Na guia/aba "Scanning" marque a opção "Suspicious files (HIPS)" para habilitar a analise por arquivos suspeitos.

| | The second second second second second second second | Contraction of the second second | ciocinat |
|--------------------------------------|--|----------------------------------|------------|
| Scanning | Extensions | Windows | Exclusions |
| Check files on | | | |
| ✓ <u>R</u> ead | | | |
| 🗸 Re <u>n</u> ame | | | |
| ✓ Write | | | |
| 5can for | | | |
| Adware and PUAs | 5 | | |
| Suspicious files | | | |
| | | | |
| Other scanning option | ns | | |
| Allow access to di | rives with infected <u>b</u> o | iot sectors | |
| Scan inside archiv | e files (not recomme | nded) | |
| 🔽 Scan system mem | iory | | |
| | | | |
| | | | |
| | | | |
| | | | |

4.1.5. Na guia "Cleanup", marque a opção "Automatically clean up item that contain a vírus/spyware", e selecione as ações que devera ser usadas caso o cleanup não esteja disponível ou caso a opção de cleanup não esteja marcada, como o exemplo da imagem abaixo:

| access scan setting | IS | | | |
|---|--------------------------|------------------------|------------|--|
| Scanning | Extensions | Windows | Exclusions | |
| Mac Exclusions | Linux/UNIX Excl | usions | Cleanup | |
| Viruses/spyware | | | | |
| 🔽 Automatically cle | an up items that contai | n a <u>v</u> irus/spyw | /are | |
| If you do not use automatic cleanup, or if cleanup is not possible, what do you want to do with the infected file? | | | | |
| • Deny access only | , | | | |
| ○ Dele <u>t</u> e | | | | |
| O Deny access and | move to default location | on | | |
| O Deny access and move to (enter a full UNC path): | | | | |
| | | B | rowse | |
| Suspicious files | | | | |
| • Deny access only |] | | | |
| O Delete | | | | |
| C Deny access and move to default location | | | | |
| O Deny access and move to (enter a full UNC path): | | | | |
| | | В | rowse | |
| | | ОК | Cancelar | |



- 4.1.6. Clique no botão "OK".
- 4.1.7. Em "Enable behavior monitoring" clique em "configure..."

| Aguionza | ation | |
|---|-----------------------|-------------|
| <u>M</u> essag | ing | |
| Sophos Live P | Prote <u>c</u> tion | |
| On-access scann | ning | |
| Enable on-acc | cess scanning | Configure |
| ✓ Enable beha⊻ | ior monitoring | [Configure] |
| Web protection | | |
| Bloc <u>k</u> access to m | alicious websites: | On 💌 |
|) ownload scannir | nn: As on-access scan | ning 💌 |
| Name | | |
| | | |
| | | |
| | | |
| A <u>d</u> d | Edit | e |
| A <u>d</u> d E <u>x</u> tensions and | Edit Remov | e |

4.1.8. Em Buffer Overflows, habilite a opção "Alert only, do not block" e clique no botão "OK".

| Configure Behavior Monitoring | × | | | | |
|---|---|--|--|--|--|
| Malicious and Suspicious Behavior (HIPS) Specify whether to detect and block program behavior | | | | | |
| that is known or suspected to be malicious. | | | | | |
| Detect malicious behavior | | | | | |
| Detect malicious traffic | | | | | |
| Detect suspicious behavior | | | | | |
| Alert only, do not block suspicious behavior | | | | | |
| Buffer Overflows | | | | | |
| Detect buffer overflows | | | | | |
| Alert only, do not block | | | | | |
| Changes only affect newly-started processes. You should restart the computer to make sure any changes made are applied. | | | | | |
| OK Cancel | | | | | |

4.1.9. Aplique as alterações clicando no botão "OK".



4.2. Firewall



- 4.2.1. No quadro "Policies", expanda o item "Firewall".
- 4.2.2. Clique com o botão direito na política "Default" (dentro o item "Firewall") e clique em "View/Edit Policy".



- 4.2.3. Na tela "Welcome to the firewall policy wizard", clique em "Avançar"
- 4.2.4. Na tela "Configure firewall", escolha a opção "Single location" e clique em "Avançar"
- 4.2.5. Na tela "Operational mode", escolha a opção "Monitor" e clique em "Avançar"
- 4.2.6. Na tela "File and printer sharing", escolha a opção "Allow file and printer sharing' e clique em "Avançar"
- 4.2.7. Clique em "Concluir" para finalizar o assistente



4.3. Tamper protection

O Tamper protection impede que usuários não autorizados editem as políticas bem como desinstalar o Sophos Endpoint do computador, com isto, será necessário informar uma senha que foi previamente configurada nas políticas da console.

| Policies |
|--------------------------|
| 🕀 📿 Updating |
| 🗄 🕢 Anti-virus and HIPS |
| 🗄 🕂 🔚 Firewall |
| Ē |
| 🗄 🗂 Application control |
| 🗄 📄 Data control |
| 🕀 🖉 Device control |
| 🕀 🗐 Full disk encryption |
| 🖻 🚫 Tamper protection |
| |
| 📴 🖶 Patch |
| 🗄 😑 Web control |

- 4.3.1. No quadro "Policies", expanda o item "Tamper protection".
- 4.3.2. Clique com o botão direito na política "Default" (dentro o item "Tamper protection") e clique em "View/Edit Policy".
- 4.3.3. Marque a opção "Enable tamper protection".
- 4.3.4. Clique no botão "Set...".
- 4.3.5. Em "Password", informe a senha desejada.
- 4.3.6. Em "Confirm password", confirme a senha e clique no botão "OK".
- 4.3.7. Clique no botão "OK".

| Tamper Protection Policy - Default | × | | | |
|--|---|--|--|--|
| Enable tamper protection | | | | |
| Create or change the password that allows endpoint users to uninstall, disable, or re-configure Sophos Endpoint Security and Control. | | | | |
| Password: | | | | |
| ••••• | | | | |
| <u>Set</u> | | | | |
| | | | | |
| | | | | |
| OK Cancel | | | | |



4.4. Patch

Atualmente, 90% dos ataques podem ser evitados com um patch existente. No entanto, muitos computadores continuam em risco, pois identificar os computadores que estão sem um determinado patch pode ser uma tarefa difícil. Alem de identificar os computadores que estão sem algum patch de correção, o Sophos Patch Assessment qualifica os patchs e identifica as ameaças que exploram a vulnerabilidade que o patch pode corrigir.



- 4.4.1. No quadro "Policies", expanda o item "Path".
- 4.4.2. Clique com o botão direito na política "Default" (dentro o item "Path") e clique em "View/Edit Policy".
- 4.4.3. Marque a opção "Enable patch assessments".
- 4.4.4. Em "Assess for missing patchs", selecione "Every day".
- 4.4.5. Clique no botão "OK"

| Patch Policy - Default | | × | | |
|---|-----------|----|--|--|
| Enable patch assessments | | | | |
| Assess for missing patches: | Every day | • | | |
| Once enabled, patch assessments occur immediately on computers and then at the interval selected. | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | OK Canc | el | | |



5. Instalando os endpoints (deploy)

Existem várias formas para realizar a instalação do software do endpoint, no entanto não é necessário realizar todas as opções. Para fazer o deploy, consulte o artigo AA-00218 em nossa base de conhecimentos, que descreve alguns métodos de deploy recomendados:

http://suporte.m3corp.com.br/article/AA-00218